A. General Information

1. **Applicability** remains the same as in the proposed rule – health plans, health care clearinghouses, health care providers; rule now cites specific exclusions made in the Privacy rule
2. **Compliance Date** = April 21, 2005 for most; April 21, 2006 for small health plans
3. Numbering has been integrated with other final rules. Proposed §142 numbering replaced by §160, §162 and §164.
4. **Scope** narrowed to electronic protected health information (ePHI) only.
5. New definitions for hybrid entity and affiliates are included in the rule. Clarification is provided on requirements for group health plans and business associates.
6. Rule is divided into Standards and Implementation Specifications. Compliance with Standards is mandatory. Compliance with Implementation Specifications may be mandatory ("required") or left to the discretion of the covered entity ("addressable").
7. Addressable Implementation Specifications require the covered entity to analyze the reasonability and appropriateness of the control given the size, complexity and capabilities of the organization, the technical environment, costs and probability/criticality of potential risks to the ePHI. Based on the analysis the entity must:
    a. If reasonable and appropriate, implement the control;
    b. If not reasonable and appropriate,
        - Document the rationale behind the decision
        - Implement an equivalent alternative measure if reasonable and appropriate.

B. §164.306 Security Standards – General Rules

1. **General Requirements:** Covered entities must:
    - Ensure CIA of all ePHI that is created, received, maintained or transmitted by the entity
    - Protect against reasonably anticipated threats or hazards to security or integrity of the ePHI
    - Protect against reasonably anticipated uses or disclosures that are not permitted under subpart E
    - Ensure compliance by the workforce.
2. **Flexibility of approach:**
    - Covered entities may use any security measures that allow reasonable and appropriate implementation of standards/specifications
    - In deciding which security measures to use, covered entities should take into account
        – size, complexity, and capabilities of the organization;
        – technical infrastructure, hardware and software security capabilities;
        – costs of security measures;

– probability and criticality of potential risks to ePHI.

3. Standards: Covered entities must comply with the standards with respect to all ePHI

4. Implementation Specifications: Covered entities must implement required and addressable implementation specifications (as previously discussed in General Information above)

5. Maintenance: Covered entities must review and modify security measures as needed to continue provision of reasonable and appropriate protection of ePHI

C. §164.308 Administrative Safeguards

1. **Security Management Process** - Covered entities must implement policies and procedures to prevent, detect, contain and correct security violations. Implementation Specifications include:
   - Risk Analysis (Required) - Assess potential risks and vulnerabilities to confidentiality, integrity and availability of ePHI
   - Risk Management (Required) - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306 Security Standards - General Requirements.
   - Sanction Policy (Required) - Apply sanctions for failure to comply with policies and procedures.
   - Information System Activity Review (Required) – Implement procedures to regularly review records of system activity (logs, access reports, security incident **tracking reports)**
2. **Assigned Security Responsibility** - Covered entities must identify an official who is responsible for development/implementation of security policies/procedures.
3. **Workforce Security** – Covered entities must implement policies/procedures to assure appropriate access and prevent unauthorized access to ePHI. Implementation Specifications include:
   - Authorization and/or Supervision (Addressable) – Implement procedures for authorization and/or supervision of workforce members working with ePHI or in locations where it might be accessed.
   - Workforce Clearance Procedure (Addressable) – Implement procedures to determine that workforce member access is appropriate.
   - Termination Procedures (Addressable) – Implement procedures for terminating access upon termination or if access is not appropriate.
4. **Information Access Management** - Covered entities must implement policies/procedures for authorizing access to ePHI where consistent with the Privacy rule. Implementation Specifications include:
   - Isolating Healthcare Clearinghouse Functions (Required) – If a clearinghouse is part of a larger organization, the clearinghouse must implement policies/procedures to protect ePHI from unauthorized access by the larger organization.

- Access Authorization (Addressable) – Implement policies/procedures for granting access to ePHI (includes access via workstation, transaction, program, process or other mechanism).
- Access Establishment and Modification (Addressable) – Implement policies/ procedures to establish, document, review and modify user's right of access to workstation, transaction, and program, process.

5. Security Awareness and Training - Covered entities must implement security awareness and training for all members of the workforce. Implementation Specifications include:

- Security Reminders (Addressable) – Implement periodic security updates
- Protection from Malicious Software (Addressable) – Implement procedures for guarding against, detecting and reporting
- Log-in Monitoring (Addressable) – Implement procedures for monitoring log-in attempts and reporting discrepancies
- Password Management (Addressable) – Implement procedures for creating, changing and safeguarding passwords

6. Security Incident Procedures - Covered entities must implement policies and procedures to address security incidents. Implementation Specifications include:

- Response and Reporting (Addressable) – identify and respond to suspected or known security incidents; mitigate, to the extent practicable; document security incidents and their outcomes.

7. Contingency Plan – Covered entities must establish (and implement as needed) policies/procedures for responding to emergencies or other occurrence that damages systems containing ePHI. Implementation Specifications include:

- Data Backup Plan (Required) – Implement procedures to create/maintain retrievable exact copies of ePHI
- Disaster Recovery Plan (Required) – Implement procedures to restore any loss of data
- Emergency Mode Operations Plan (Required) - Implement procedures to enable continuation of critical business processes for protection of security of ePHI while operating in emergency mode.
- Testing and Revision Procedures (Addressable) – Implement procedures for periodic testing and revision of plans
- Applications and Data Criticality Analysis (Addressable) - Assess relative criticality of applications and data in support of other contingency plan requirements.

8. Evaluation – Covered entities must conduct periodic technical and non-technical evaluation to establish the extent to which security policies/procedures meet requirements. Evaluations must be conducted:

- Initially, based on the HIPAA Security rule
- In response to environmental or operational changes affecting security of ePHI.

9. Business Associate Agreement – Covered entities may permit business associates to create, receive, maintain or transmit ePHI on their behalf if it receives sufficient assurance that the business associate will appropriately safeguard information.

Final Security standards are excerpted from The Federal Register, Vol. 68, No. 34, Thursday, February 20, 2003..

This standard excludes:

- transmissions from a covered entity to a provider for treatment purposes;
- transmission of ePHI by a group health plan, HMO or health insurance issuer to a plan sponsor to the extent that group health plan requirements (§164.504(b)) applies;
- transmission of ePHI from or to other agencies providing service when the covered entity is a government public health program that does not perform the eligibility or enrollment task for the services.

Violation of the security assurances constitutes non-compliance. Implementation Specifications include:

- Written Contract or Other Arrangement (Required) - Documentation of assurances or other arrangement that meets applicable requirements is required.

D. §164.310 Physical Safeguards

1. Facility Access Controls – Covered entities must implement policies/procedures to limit physical access to electronic Information Systems and the facility/facilities where they are housed, while allowing properly authorized access. Implementation Specifications include:

- Contingency Operations (Addressable) – Implement procedures that allow access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan.
- Facility Security Plan (Addressable) – Implement policies/procedures to safeguard the facility and equipment from unauthorized access, tampering or theft.
- Access Control & Validation Procedures (Addressable) – Implement procedures to control/validate person's access to facilities based on role/function, including visitor control, and control of access to software programs for testing and revision.
- Maintenance Records (Addressable) – Implement policies/procedures to document repairs/modifications to physical components of the facility, which are related to security (e.g. hardware, walls, doors, locks).

2. Workstation Use – Covered entities must implement policies/procedures that specify proper function, manner functions are performed & physical attributes of surroundings of a specific workstation or class or workstations that can access ePHI.

3. Workstation Security – Covered entities must implement physical safeguards for all workstations that access ePHI (to restrict access to authorized users).

4. Device and Media Controls – Covered entities must implement policies/procedures to govern receipt and removal of hardware/electronic media that contain ePHI – into, out of and within the facility. Implementation specifications include:

- Disposal (Required) - Implement policies/procedures for final disposition of ePHI and/or hardware/media on which it resides.
- Media Re-use (Required) – Implement procedures for removal of ePHI from electronic media before media is available for re-use.

- Accountability (Addressable) - Maintain record of movement of hardware and electronic media and any person responsible therefore.
- Data Backup/Storage (Addressable) - Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

E. §164.312 Technical Safeguards

1. Access Control –Covered entities must implement technical policies/procedures for electronic Information Systems that maintain ePHI to allow access only to authorized persons or programs. Implementation Specifications include:

- Unique User Identification (Required) - Assign a unique name/number for identifying and tracking user identity.
- Emergency Access Procedure (Required) – Implement procedures for obtaining necessary ePHI during an emergency.
- Automatic Logoff (Addressable) – Implement electronic procedures that terminate an electronic session after a pre-determined period of inactivity.
- Encryption and Decryption (Addressable) – Implement a mechanism to encrypt and decrypt ePHI.

2. Audit Controls – Covered entities must implement hardware, software or procedural mechanisms that record and examine activity in Information Systems containing ePHI.

3. Integrity – Covered entities must implement policies/procedures to protect ePHI from improper alteration or destruction. Implementation Specifications include:

- Mechanism to Authenticate ePHI (Addressable) – Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

4. Person or Entity Authentication – Covered entities must implement procedures to verify that a person or entity seeking access to ePHI is who he/she/it claims to be.

5. Transmission Security – Covered entities must implement technical measures to guard against unauthorized access to ePHI being transmitted over electronic networks. Implementation Specifications include:

- Integrity Controls (Addressable) – Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
- Encryption (Addressable) – Implement a mechanism to encrypt ePHI whenever deemed appropriate.

F. §164.314 Organizational Requirements

1. Business Associate Contracts or Other Arrangements – A covered entity:

- Must meet implementation specification requirements.
- Is not in compliance if aware of a pattern of activity or violation of business associate's contract obligations, unless reasonable steps are taken to cure breach or end violation. If steps taken to cure/end violation are unsuccessful, the covered entity must:

- Terminate contract or
- If termination not feasible, report problem to the Secretary.

Implementation Specifications are mandatory and include:

- Business Associate Contract – The contract must provide that business associate will:
  - Implement administrative, physical, technical safeguards that reasonably/appropriately protect CIA of ePHI that it creates, receives, maintains or transmits on behalf of covered entity.
  - Ensure that any agent, including subcontractors, to whom it provides information agrees to implement reasonable and appropriate safeguards to protect ePHI.
  - Report to covered entity any security incident it becomes aware of.
  - Authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.
- Other Arrangements – When the covered entity and business associate are government agencies, the covered entity is compliant if:
  - There is a Memorandum of Understanding with the business associate containing terms that accomplish objectives of a business associate contract.
  - Another law (including agency-adopted regulations) accomplishes the objectives of the business associate contract.
    A covered entity may permit the business associate to create, receive, maintain or transmit ePHI on its behalf to the extent necessary for the legal mandate without a contract if the business associate is required by law to perform a function or activity on behalf of covered entity or provide a service as described in the business associate definition.
    The covered entity may omit the termination clause from the arrangements authorization if it is inconsistent with statutory obligations of the covered entity or business associate.

2. Requirements for Group Health Plans – A Group Health Plan must ensure that plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained or transmitted to or by the plan sponsor on behalf of the group health plan.

- Implementation Specifications (Required) - Plan documents must be amended to incorporate provisions to require plans sponsor to:
  - Implement administrative, physical, technical safeguards that reasonably/appropriately protect the confidentiality, integrity and availability of ePHI that it creates, receives, maintains or transmits on behalf of the group health plan;
  - Ensure adequate separation is supported by adequate security;
  - Ensure that agents implement security measures;
  - Report to security incidents to the group health plan.

G. §164.316 Policies, Procedures and Documentation Requirements

1. Policies and Procedures – Covered entities must implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications or other requirements.

- Covered entities must take the General Requirements into account.
- Policies/procedures can be changed, but change must be documented and implemented in accordance with regulations.

2. Documentation – Covered entities must maintain policies/procedures in written form (may be electronic); document action, activity, assessments as required (may be electronic). Implementation Specifications include:

- Time Limit (Required) - Retain documentation for 6 years from create date or last effective date, whichever is later.Availability (Required) - Make documentation available upon request to those responsible for implementation of security procedures.Updates (Required) - Periodically review and update documentation as needed in response to environmental/operational changes affecting security of ePHI.

[1] Final Security standards are excerpted from The Federal Register, Vol. 68, No. 34, Thursday, February 20, 2003..